PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

To:

PERSSON, Michael
Lawson, Philpot & Persson, P.C.
67 Water Street, Suite 110
Laconia, NH 03246
ETATS-UNIS D'AMERIQUE

Date of mailing (day/month/year) 20 July 2000 (20.07.00)	
Applicant's or agent's file reference	**IMPORTANT NOTIFICATION**
International application No. PCT/US99/21663	**International filing date** (day/month/year) 17 September 1999 (17.09.99)

1. *The following indications appeared on record concerning:*

☐ the applicant ☐ the inventor ☒ the agent ☐ the common representative

Name and Address	State of Nationality	State of Residence
PERSSON, Michael Law Offices of William B. Ritchie 72 N. Main Street Concord, NH 03301 United States of America		
	Telephone No. 603-225-5212	
	Facsimile No. 603-225-5146	
	Teleprinter No.	

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

☐ the person ☒ the name ☒ the address ☐ the nationality ☐ the residence

Name and Address	State of Nationality	State of Residence
PERSSON, Michael Lawson, Philpot & Persson, P.C. 67 Water Street, Suite 110 Laconia, NH 03246 United States of America		
	Telephone No. 603-528-2900	
	Facsimile No. 603-528-1117	
	Teleprinter No.	

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

☒ the receiving Office
☐ the International Searching Authority
☒ the International Preliminary Examining Authority
☐ the designated Offices concerned
☒ the elected Offices concerned
☐ other:

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer I. Britel
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

PATENT COOPERATION TREATY

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:

PERSSON, Michael J.
LAWSON , PHILPOT & PERSSON P. C.
67 Water Steet, Suite 110
Laconia, NH 03246
ETATS-UNIS D'AMERIQUE

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL PRELIMINARY EXAMINATION REPORT
(PCT Rule 71.1)

Date of mailing *(day/month/year)*	29.11.2000
Applicant's or agent's file reference: 1270-028	**IMPORTANT NOTIFICATION**

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US99/21663	17/09/1999	29/09/1998

Applicant
KAWAGUCHI, Eiji et al.

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.

2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.

3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.

4. **REMINDER**

The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices) (Article 39(1)) (see also the reminder sent by the International Bureau with Form PCT/IB/301).

Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

Name and mailing address of the IPEA/	Authorized officer
European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Slater, S Tel.+49 89 2399-2565

Form PCT/IPEA/416 (July 1992)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
1270-028		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US99/21663	17/09/1999	29/09/1998
International Patent Classification (IPC) or national classification and IPC G06K19/07		
Applicant KAWAGUCHI, Eiji et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 24 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☐ Certain documents cited
   - VII ☒ Certain defects in the international application
   - VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
25/04/2000	29.11.2000
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Heusler, N Telephone No. +49 89 2399 2359

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/US99/21663

I. Basis of the report

1. This report has been drawn on the basis of *(substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments (Rules 70.16 and 70.17).)*:
Description, pages:

1,1a-1b,2,4,5,5a, 6,6a,7-18	as received on	20/11/2000	with letter of	15/11/2000

Claims, No.:

1-15	as received on	20/11/2000	with letter of	15/11/2000

Drawings, No.:

1-7	as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

   These elements were available or furnished to this Authority in the following language: , which is:

   - ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
   - ☐ the language of publication of the international application (under Rule 48.3(b)).
   - ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

   - ☐ contained in the international application in written form.
   - ☐ filed together with the international application in computer readable form.
   - ☐ furnished subsequently to this Authority in written form.
   - ☐ furnished subsequently to this Authority in computer readable form.
   - ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
   - ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

   - ☐ the description, pages:

☐ the claims, Nos.:

☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

   (Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-15
	No:	Claims	
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-15
Industrial applicability (IA)	Yes:	Claims	1-15
	No:	Claims	

2. Citations and explanations
   see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:
see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:
see separate sheet

The following documents are cited:

D1: US - A - 5 636 292
D2: EP - A - 0 334 616
D3: US - A - 5 689 587
D4: EP - A - 0 638 880

Ad V.2 - novelty, inventive step; citations and explanations

1. The application **relates to** an information card (f.e. credit card) where user data (for instance a photograph or the voice of the bearer in a digitized form) are stored in a card memory. Such cards also store a password enabling only the authorized user to operate the card. There is the **problem** that this password may illegally be obtained by reading out the card memory.

   The **solution** is to provide the password (the "data that authenticates the legitimacy of the card owner") in the form of "inherent data", i.e. hidden in the image or sound data (imperceptible) by means of "steganography", i.e. embedding, digital watermarking, or digital picture envelope technology (BPCS steganography: replacing a random pattern of image data with secret data). Even if a third party is able to read the information data from the card, since the inherent data is hidden in the information data, the third party cannot recognize the presence of the secret data. Without a customized key, it is not possible to know where and how the secret data can be extracted. Thus it is possible to provide the information card with a high level of security. It is possible to hide the presence of card owner data and the legitimacy data.

2. Closest **prior art** D1 discloses an information card ... that stores information data including image data (see fig. 24 and col. 57, from line 30), ... wherein the information data contains inherent data that is embedded in the information data according to steganography (col. 2, lines 11-16; col. 57, from line 30).

   According to D1, the image data is printed out on the card (col. 58, line 11); the image is read (when using the card) with a CCD scanner (see bottom of col. 59).

   D1 is silent on whether a memory is present in the card. It is, however, well known to a skilled person to include a memory in such a card, and to store the image into that memory. D2 discloses such a card (col. 5, lines 6/7 and lines 27-36).

   D1 also discloses that the inherent data is data that authenticates the legitimacy of a card owner of the information card: According to D1, a PIN number is used to legitimate the user (col. 60, lines 10-14). The PIN creates "formidable obstacles to a thief using that card" (col. 57, from line 50).

Since a combination of D1 and D2 leads the skilled person to a device within the scope of **claim 1**, this claim does not comply with Art. 33 (3) PCT.

It is noted that also D4 discloses a data card with a memory (page 4, lines 35-37), where fake-proof video information is stored in the memory (page 4, lines 39-41). D4 also suggests to verify authenticity of the user (page 3, line 24).

3. As to the dependent claims:

Claims 2, 3, 6-11, 14 and 15 add features well known in the field of information cards or even disclosed in D1 or D2. These claims add nothing inventive.

The other claims merely define straightforward embodiments and possibilities from which the skilled person would select, in accordance with circumstances, without the exercise of inventive skills, in order to solve the problem posed. As an example, **claims 4, 5, 12 and 13** define mathematical details as to encoding the secret information. These steps are disclosed or suggested by the prior art on hand, see for example D3. Moreover the description does not make clear what specific advantages these additional features might imply. Therefore these claims add nothing inventive.

Finally, the dependent claims are obviously not linked by one single general inventive concept (Rule 13 PCT).

4. D3 discloses mathematical basics on steganography without suggesting the use in a data card.

Ad VII. - certain defects (form and content, Rules 5 - 7 PCT)

The independent claims are in the two-part-form (Rule 6.3b PCT), but it is not clear from the description against which document the claims are delimited. **Claim 1** appears not to be delimited against D1.

Ad VIII. - clarity, conciseness, support by th description (Art. 6 PCT):

1. The formulation "one of ... and ..." in **claims 1, 4, 12** is unclear and lacks conciseness.

2. The term "steganographic" in **claim 1** and other claims is not understandable. This word is, for example, not included in "The Concise Oxford Dictionary".

3. The formulation "one of ..., both formed" in **claims 4 and 12** is not clear.

4. It is not clear what the expression "conjugation operation" in **claims 5 and 13** means. Claims should be clear without the description.

5. In **claim 8** it is unclear whether the two passwords mentioned here are the same.

6. It is not clear what passwords are meant in **claim 10**.

7. **Claims 12 to 15** lack conciseness, since these claims correspond to claims 4 to 7.

INFORMATION CARD AND INFORMATION CARD SYSTEM

BACKGROUND OF THE INVENTION

1. Field to which the Invention Pertains

The present invention relates to an information card and an information card system. More particularly, it relates to an information card for use as a credit card, a cash-vending card, an ID card, etc. which employs Steganography, i.e., image data embedding, digital watermarking, information hiding, or digital picture envelope technology, and further to an information card system employing such an information card.

2. Description of Related Art

One known type of the information card is heretofore an IC card for use as, e.g., a credit card and an ID card. The IC card has an IC chip mounted on a plastic plate. The IC chip has either a microprocessor and a memory or a memory only. The IC card with the IC chip having both of the microprocessor and the memory is what is called an IC card, while the IC card with the IC chip having only the memory Is termed as a memory card.

The IC card for use as the credit card carries on its plastic plate surface the name of the card owner and the card number. The memory (ROM) in the IC chip stores an authentication program, a password, and so on. In some cases, the authentication program and the password for use by the authentication program are encrypted for protection against unauthorized access.

However, such conventional IC cards do not have a sufficient level of security. More specifically, there have been cases where someone illegally obtains the password or decodes the encrypted data, and thereby illegally use the IC card. In addition, attempts have been made to forge the IC card as a whole. The use of such a forged IC card cannot be prevented once the password is obtained.

United States Patent No. 5,636,292 discloses steganography methods employing embedded calibration data in which an identification code signal is impressed on a carrier to be identified in a manner that permits the identification signal later to be discerned and the carrier thereby identified. The method and

apparatus are characterized by robustness despite degradation of the encoded carrier, and by permeation of the identification signal throughout the carrier. In some embodiments, the methods are utilized in order to embed a signal on a personal cash card, onto which is disposed a photograph of the card owner, in a manner that the card may be identified via interaction with a remote computer network.

European Patent Number 334,616 discloses a method and system that utilize a private key of a public-key cryptosystem key pair to encrypt a non-secret password into a digital signature. The password and the digital signature are then encoded and stored on a magnetic stripe or other memory device of the card. To effect a transaction, the digital signature on a received card must be shown to have been generated from the password on the received card. The password preferably includes a digitized photograph of the authorized cardholder which is capable of being displayed at the transaction terminal. This enables the operator of the terminal to verify the identity of the cardholder by visual inspection.

United States Patent Number 5,689,587 discloses a method and apparatus for data hiding in images which increases and decreases parameter values at randomly selected host image locations assigned to respective first and second groups. The alteration modifies the statistical behavior of a test statistic equivalent to a linear combination of a large number of instances of respective functions, associated with the pattern, of the parameter values at first and second group locations. The presence or absence of the pattern in a test image is determined by comparing the experimental value of the test statistic associated with the pattern with the expected value of the same sum for an unaltered host image.

European Patent Number 638,880 discloses a card verification system that allows for the reading of data from an EEPROM memory device. A photographic type image is stored in the memory device. The data comprises a data table containing randomly distributed unique serialized information and desired verification data is downloaded from a central processing system. The system uses color cell compression for the acquisition, digitization and compression of the photographic-type image, which may be a facial representation, fingerprint, signature,

voice print, eye retina or any other unique personal identification in a compressed form which may read by the decoding system to verify the positive identification of the presenter.

SUMMARY OF THE INVENTION

It is therefore an object of the present invention to provide an information card and information card system which can completely be prevented from being forged. This object is achieved by the subject matter of claims 1, 4, 5, 7, & 15

Another object of the present invention is to provide an information card,

which can completely be prevented from being illegally used, and an information card system. This object is achieved by the subject matter of claims 1-3, 6, and 8 - 14.

In the present invention, as defined in claim 1, the information card contains the information data in the memory. The information data includes either image data or the acoustic data. The inherent data is embedded in the information data according to steganography. As a result, even if a third party is able to read the information data from the information card, since the inherent data is hidden in the information data according to steganography, the third party cannot recognize the presence of the inherent, secret, data. Thus, it is possible to provide the information card with a high level of security. The information data may be of such a size as to allow the inherent data to be embedded therein according to steganography. The inherent data shows the legitimacy of the card owner of the information card.

In the present invention, as defined in claim 2, since the memory contains the password for allowing the information data to be read from the memory, password checking can allow the information data to be read therefrom. Accordingly, the security of the stored information data can be made high.

In the present invention, as defined in claim 3, the use of the customized key enables the inherent data to be extracted from the information data. The customized key is not stored in the information card, and hence can be made highly safe because this key cannot be stolen.

In the present invention, as defined in claims 4 and 12, the information card contains the information data. The information data has the inherent data embedded therein according to steganography. As defined in claim 8, the information card further stores a password for permitting the information data to be read from the memory. The data processing terminal checks a submitted password against the password stored in the information card. When the submitted password identifies with the stored password, then the data processing terminal permits the information data to be read from the information card, and then outputs such retrieved information data. For example, the read information data is

displayed on a display unit, outputted as sounds, or transmitted as electronic data through a communication line.

As a consequence, the information data stored in the information card is protected against retrieval therefrom by password checking because no unauthorized persons are allowed to access it.

In the present invention, as defined in claim 9, the information card retains the information data and the inherent data and the data processing terminal extracts the inherent data from the information data by means of a submitted customized key. The data processing terminal permits the inherent data to be extracted only when the submitted customized key is a legitimate customized key. Therefore, even if a third party is aware of the presence of the embedded inherent data, the third party can be prevented from extracting the inherent data because the third party does not know the customized key, and further cannot randomly submit any key that is identical to the legitimate customized key. Accordingly, the information card system provides a high level of security.

In the present invention, as defined in claim 10, the information card contains the password other than the information data, called the inherent data . The data processing terminal protects the information data by password, and further protects the inherent data by customized key. As a result, the inherent data is protected against extraction by double protection scheme.

In the invention, as defined in claim 11, the inherent data is read from the host and put into the data processing terminal, or is submitted from the external source into the data processing terminal. The read or submitted inherent data is wholly or partly checked against the inherent data that is contained in the information card. When these inherent data identify with one another, then the information card is possible to work as it is programmed. For example, it can function as a credit card. As a consequence, the information card system provides triple security, making it possible to eliminate forgery and illegal use.

In the present invention, as claimed in claim 12, the inherent data is embedded according to Steganography by the steps of converting the information data to pure

binary code

5

data, or converting the pure binary code data to canonical gray code data, decomposing the pure binary code data or the canonical gray code data into bit planes, and segmenting the bit planes into regions according to a complexity measure, and replacing complex region-forming data with the produced inherent data. As a result, the memory of the information card stores information data that has the inherent data embedded therein. In addition, the inherent data Is hidden so that the third parties are unaware of the presence of the inherent data.

In the present invention, as defined in claims 5 and 13 the inherent data to be embedded is subject to a conjugation operation. As a result, various files can be embedded.

In the present invention, as defined in claims 6 and 14, the memory of the information card includes an IC chip. As a consequence, it is possible to build an information card, which serves as, what is called, either a memory card or an IC card, and a system of such an information card. In this case, an inexpensive card reader/writer can be provided as the data processing terminal.

In the present invention, as defined in claims 7 and 15, the information card carries a photograph on the card surface thereof. The information data or the inherent data represents the photograph. When image data is output and displayed, then such data can be checked against the photograph. This makes the information card highly secure.

BRIEF EXPLANATION OF THE DRAWINGS

FIG. 1 is a block diagram, illustrating how an information card system according to the present invention functions.

FIGS. 2(A) to 2(F) are simulative illustrations illustrative of a conjugation operation according to the present invention.

FIG. 3 is a block diagram, showing an information card system according to an embodiment of the present invention.

FIG. 4 is a block diagram, showing how the information card system according to the embodiment is electrically constructed.

FIG. 5 is a block diagram, illustrating how an information card according to

the embodiment is electrically constructed.

FIG. 6 is a flowchart, showing an embedding process (encoder program) in one embodiment of the

5

information card system.

FIG. 7 is a flowchart, showing an authentication process (decoder program) in one embodiment of the information card system.

DETAILED DESCRIPTION OF THE INVENTION

An information card system according to an embodiment of the present invention will now be described. FIG. 1 is a block diagram, showing the concept of the system according to the present invention. More specifically, the information card system includes an information card, a data processing terminal for exchanging data with the information card, and a host computer for exchanging data with the data processing terminal. The information card has a memory for storing data. The memory contains information data and a password. The information data has inherent data embedded therein by a steganographic process. The data processing terminal has input means, output means, password checking means, and inherent data extracting means.

According to the information card system, the data processing terminal can read the information data by password checking. It can also extract the inherent data using a customized key. As a result, when the information card is used as a credit card, it is possible to completely eliminate the illegal use of the information card by any person other than the legitimate card owner. Further, it is also possible to completely eliminate illegal use of a forged information card.

Since the inherent data is embedded in the information data according to Steganography (BPCS Steganography), it is possible to eliminate the card forgery and the inherent data extraction by unauthorized persons.

The BPCS-Steganography (Bit-Plane Complexity Segmentation Steganography) is a process of replacing (embedding) a random pattern of image data with secret data, in view of the complexity (randomness) of a binary pattern on a "bit plane" that is obtained, e.g., by slicing the image data into bits. Whereas a hiding capacity of a conventional steganographic process is in the range of 5 to 10%, the BPCS-Steganography has a hiding capacity of about 50% or up to some 70% in some cases. Therefore, the BPCS-Steganography is capable of hiding with a very high

hiding capacity. The BPCS-Steganography is based on the following four basic ideas:

(1)Bit-plane decomposition is executed on a pure binary coded (PBC) image data or a "canonical gray coded (CGC) image converted from the PBC image data.

(2) A bit plane is segmented according to the "complexity measure" of a binary pattern, and a complex pattern (random pattern) is replaced by the secret data (i.e., the secret data is hidden) . The secret data thus hidden is completely unnoticeable for human eyes.

(3) Files to be embedded are subject to a "conjugation operation", so that any types of files can be embedded.

(4) The algorithm of BPCS-Steganography (encoder and decoder programs) can be customized differently to different users. The customized BPCS-Steganography algorithm establishes the security of embedded information with the use of a "customized key" that is different from the password.

The most advantageous feature of the BPCS Steganography is that it can hide with a large hiding capacity. This feature is applicable to the following:
(A)Others do not become aware of that some secret data is embedded. It is also impossible to see any difference between a secret data-embedded image and a non-embedded image.
(B) Even if someone suspects that secret data might be embedded, he is unable to know, without a customized key, where and how the secret data can be extracted.

The information card system according to the present invention employs a steganographic card which has an IC memory mounted on a conventional card (with a photograph of the card owner thereon) . The IC memory has a storage capacity of 8 KB or more. The steganographic card is used as follows:

(1) The IC memory stores the data of the photograph of the card owner. In order to read this data, the password for the card must be submitted to a card reader.

(2) The data of the photograph of the card owner contains personal data regarding the card owner (e.g., fingerprints, a personal history, data of relatives, data

of hobbies, etc.). The personal data is embedded according to the BPCS-Steganography.

(3) In order to extract the embedded information and display the extracted information on a display unit, it is necessary to submit a correct customized key. The customized key is defined as follows:

(a) Only the card owner knows a portion of the customized key (a private key).

(b) The remaining portion of the customized key (a company key) is strictly and confidentially managed only by the card company. Only when the card company receives an on-line request for the company key from a facility (shop) where the card is used, the card company encrypts the company key and sends the encrypted company key to the facility. In order to recover the embedded information, the private and company keys must be combined together.

(c)The card owner is unaware of the company customized key, while the card company is unaware of the private key.

In the information card system according to the present invention, there are four levels of security confirmation as to both a legitimate card owner and a legitimate card. Each security confirmation level is as follows:

(Level 1) Visual checking of the card user against the photograph on the card (in order to prevent stolen or found cards from being illegally used)

(Level 2) Requesting the card user to submit the "password", and visually checking the photograph data displayed on the display unit against the photograph on the card (in order to prevent photographs on cards from being forged)

(Level 3) Requesting the card user to submit the "private key", combining the private key with the "company key" that is sent on-line from the card company, and confirming whether the personal data embedded according to the BPCS--Steganography can be extracted (in order to prevent cards from being forged as a whole).

(Level 4) Checking of the card user against the legitimate card owner based on the embedded personal data (e.g., fingerprints) (in order to prevent the legitimate card

owner from renting the card to others)

Hiding and extraction of information according to the BPCS-Steganography will be described below.

On the bit planes of a natural image, a noise-like area does not appreciably affect the visual appearance to the viewer even if the data therein is replaced with other noise-like data. This phenomenon allows us to replace noise-like areas in a natural image with secret data. Since a criterion to determine whether the noise-like areas varies depending upon the natural image, it is necessary to establish a suitable threshold value for each natural image data.

When a binary image is analyzed by the local area of $2^m \times 2^m$ (normally $m = 3$), and some area has a complexity measure value a which satisfies:

$$a_{th} < a$$

(where a_{th} represents a threshold), then the area is decided as an area for secret data hiding or embedding.

In order to embed a secret data file in a natural image, the secret data file may be first divided into small file segments with $2^m \times 2^m$ size (i.e., $2^m \times 2^m$ pixel size), and then those small file segments may be embedded successively in noise-like areas of the same size in the image. However, not all small file segments have a complexity value greater than a_{th}. The small file segments having less complexity value than the threshold a_{th} are converted to more complex segments by a conjugation operation described below. Such a process makes it possible to embed any secret files in images. However, in order to recover all parts of the embedded secret files, it is necessary to save the "conjugation map" which indicates the conjugated segment areas.

Now, assume that a white pixel has a value of 0, but a black pixel has a value of 1. P is assumed as an arbitrary binary image having white background. W is defined as a pattern where all pixels are white. B is taken as a pattern where all pixels are black. Wc is viewed as a checkerboard pattern where the leftmost pixel in the uppermost pixel row is white. Bc is taken as a checkerboard pattern where the leftmost pixel in the uppermost pixel row is black. (See FIGS 2a - 2f). The binary image P is regarded as an image with a foreground area having the pattern B and a

background area having the pattern W. On the basis of the above assumption, the "conjugated image" P* of the image P is defined as follows:

$$P^* = P \oplus Wc$$

where ⊕ represents an exclusive-OR operation on each pixel.

A process for producing a conjugated image is referred to as a conjugation operation. The conjugated image P* is characterized as follows:

(1) The foreground area is identical in shape to the foreground area of the image P.

(2) The foreground area has the checkerboard pattern Bc.

(3) The background area has the checkerboard pattern Wc.

The image P and the conjugated image P* have one-to-one correspondence. The image P and the conjugated image P* satisfy the following properties:

(a) $(P^*)^* = P$

(b) $P^* \neq P$

(c) $a(P^*) = 1 - a(P)$

where "a(P)" represents complexity a of the image P.

The most important of the properties (a) through (c) is the property (c) . The property (c) indicates that a simple image can be converted to a complex image or vise versa without losing its shape information. It is also possible to restore the original image from the converted image because of the property (a)

The BPCS-Steganography proposed by the present application includes the following five steps:

Step 1:

A natural image of $2^M \times 2^M$, N bits/pixel is converted to an N-bit gray code image. This conversion step is based on the study by Eiji Kawaguchi et al. of binary images produced by bit-plane decomposition and their complexity.

Step 2

The gray code image generated in Step 1 is segmented into N binary images by bit-plane decomposition.

Step 3

Each of the N binary images is divided into partial images each having a size of $2^m \times 2^m$. The partial images are represented by P_i; i = 1, 2, ···, 4^{M-m} The nth bit-plane image can be expressed by:

$$I_n = \{P_1^n, P_2^n, \cdots, P_{4^{M-m}}^n\}$$

Similarly, the nth "conjugation map" can be expressed as follows:

$$C_n = \{Q_1^n, Q_2^n, \cdots, Q4^n_{M-m}\}$$

where each of $Q_1^n, Q_2^n, \cdots, Q4^n_{M-m}$ has a value of "0" or "1." The value of "1" represents an area where the conjugation operation is applied. The value of "0" represents an area where the conjugation operation is not applied.

Embedded data (expressed by E) includes a header, a body, and a pad. The header indicates a data size of the body. The body represents secret data (e.g., a secret image) which is embedded. The pad serves to shape the embedded data into the size of $2^m x 2^m$. E_j (j=1,2,···,J) represents a partial bit series of the embedded data E whose size is of $2^m x 2^m$ bits. When the partial bit series E_j is corresponded to a square area of $2^m x 2^m$ bit by bit, based on the principle of raster scanning, then a binary image of $2^m x 2^m$ can be generated. The generated binary image is represented by makeS(E_j).

With the threshold a_{TH} used, an embedding algorithm can be expressed below. Each Q in the nth conjugation map C_n is initialized to "0".

```
for (n=N, j=1;n≥1&&j<J;n--) {

    for (i=1;i≤4^(M-m)&&j<J;i++) {

        if (a(P_i^n)≥a_TH) {

            if (a(makeS(E_j))≥a_TH)

                P_i^n = makeS(E_j)
            else {
```

$P_i^n = makeS(E_j)^*$

$Q_i^n = "1"$

}

j++

Since low-order bits are less significant on the image, the embedding process is carried out on bits successively from the least significant bit. When the binary image makeS (E_j) in an area is simple, i.e., when the complexity of the area is smaller than the threshold, then the conjugation operation is effected on the binary image makeS (E_j). In this case, Q_j in the conjugation map is set to "1."

Step 4

The N-bit gray code image is reconstructed from the N binary images where the secret data is embedded.

Step 5

After the N bit pure binary code is recovered from the N-bit gray code image in Step 4, the image data file having the secret data embedded therein is obtained.

The secret data embedded in an image may be recovered by the above algorithm being reversed. In order to recover the secret data from the embedded image, it is necessary to know the threshold a_{TH} and the conjugation map.

Next, an IC card system according to an embodiment of the present invention will be described with reference to FIGS. 3 to 7. FIG. 3 is a block diagram, showing the concept of the IC card system. FIG. 4 is a block diagram, illustrating a schematic structure of an IC card and an IC card reader/writer in the ID card system. FIG. 5 is a block diagram, illustrating another structural example of an IC card. FIGS. 6 and 7 are flowcharts, showing programs to be executed in the ID card system.

As shown in the above Figures, an IC card 100 as an information card according to the present invention is capable of exchanging data with an IC card reader/writer (data processing terminal) 200. The IC card reader/writer 200 can exchange data on-line with, e.g., a host computer 300 at a credit card company. The IC card reader/writer 200 may be equipped with a display unit 210 (display means) and an input means 220 (such as a mouse and a keyboard).

As shown in FIG. 4, the IC card reader/writer 200 includes a CPU to execute arithmetic operation processing, a data memory for storing data, a program memory for storing programs, a buffer memory, the keyboard for entering data, a display unit for displaying results of the arithmetic operation processing, an interface for controlling data exchanged with the IC card, and a power supply.

The IC card reader/writer 200 is able to read data from and write data in the IC card 100. The CPU executes encrypting and decrypting processes and an authentication process. The program memory stores application programs.

The IC card 100 has an interface, a CPU, a program memory, and a data memory. The power supply of the IC card reader/writer 200 supplies electric power to the IC card 100.

The program memories and the data memories are nonvolatile types. These nonvolatile memories include EEPROMs that is electrically erasable, or static RAMs that is backed up by a battery.

FIG. 5 shows another structural example of an IC card. More specifically, the IC card includes a CPU, a PROM for storing data, and a connector for connection to an external device (an IC card reader/writer). The CPU includes a control unit, an arithmetic unit, a ROM, and a RAM.

The IC card includes an IC chip that is mounted on a plastic plate member. The plastic plate member carries the name of the card owner, the card number, and an expiration date, all of which are embossed on a surface thereof.

The IC chip stores, in a memory thereof having a storage capacity of 8 KB or more, password data, digital image data of the card owner's photograph, or digital acoustic data (information data). The information data contains personal data of the card owner (e.g., fingerprints), a photograph of the card owner, and part of the personal data (digital signature image data), all of which are embedded according to the BPCS-Steganography.

The IC card system enables both visual verification of the card user and mechanical authentication of the IC card at one time. People cannot perceive any secret present in the IC card. Even if someone suspects some secret data as being present in the IC card, they cannot extract such an embedded data from the IC card. The IC card may hide digital data

or authentication data. The IC card system can properly readout such hidden authentication data from the IC card, and properly can embed the same data therein.

FIG. 6 shows a process (encoder program) in which data is stored in the IC card according to Steganography. Initially, the card owner's photograph data (including indexed photograph data) is produced in order to be written to the IC card memory (8KB or more). The produced photograph data is saved as a bit map file. In this case, the photograph data is set in size to be some 75% of the IC card memory. In addition, the above photograph data is produced from the photograph data of the IC card owner.

Then, personal authentication data (text data) is produced and then saved in order to be embedded in the photograph data. The text data is set in size to occupy some 10% of the photograph data. Both of the photograph data and the authentication data are selected and displayed. Then, the photograph data for the IC card is converted to pure binary code (PBC) data. The photograph data thus converted to the PBC data is then converted to canonical gray code (CGC) data.

Next, the photograph data thus converted to the CGC data is decomposed into bit planes (i.e., into N binary images). The personal authentication data (text data) is embedded in the bit-plane-decomposed photograph data. In this case, the personal authentication data is embedded according to the above algorithm, using a customized key (which consists of, e.g., 24 digits of data).

The photograph data having the embedded text data therein is then re-converted to PBC data. Further, the photograph data for use in the IC card is produced and then saved.

Now, the IC card is inserted into the IC card reader/writer, and then any one of the photograph data is selected. Then, the selected photograph data is transferred and saved in the IC card memory. In order to protect the saved photograph data, a password is set and saved in the IC card memory. The password consists of, e.g., 4 digits of data.

The IC card (for use as, e.g., an identification card) is now completed. Thereafter, a photograph of the card owner is printed out on the plastic plate surface of the IC card.

Next, the authentication of the IC card will be described with reference to FIG. 7. FIG. 7 shows part of a decoder program.

Initially, the IC card is inserted into the IC card reader/writer. Then, the IC card reader/writer starts an initializing process in order to execute an authentication flow. Next, a password is submitted from a keyboard into the IC card reader/writer. The IC card reader/writer compares the submitted password with the stored password in the memory on the IC card. When the submitted password identifies with the stored password, then the IC card reader/writer reads the photograph data (information data) stored in the IC cardmemory, and displays it on the display unit. When the displayed photograph data indicates a photograph of the card owner, then the displayed photograph is visually checked against the photograph printed on the IC card surface and against the card user himself.

Then, a customized key is submitted. The customized key is used to embed the personal authentication data. The customized key is known only to the legitimate card owner. The customized key is not stored in the IC card memory. The customized key works as parameters to control over embedding and extracting of the inherent data. The inherent data is extracted from the information data only when the customized key submitted to extract the inherent data identifies with parameters that are used for embedding.

More specifically, the photograph data (information data) read from the IC card memory is converted to pure binary code (PBC) data, and then the photograph data thus converted to the PBC data is converted to canonical gray code (CGC) data. The CGC data of the photograph is decomposed into bit-planes. At this time, the personal authentication data is extracted from the photograph data already decomposed into the bit-planes, using the customized key. In this manner, the embedded personal authentication data (text data) is extracted from the photograph data, and is then displayed.

When the submitted password does not identify with the password in the IC card memory, then no photograph data can be read from the IC card memory. Further, when the submitted customized key does not identify with the card owner's customized key, then the personal authentication data cannot be extracted from the photograph data. In case such a password or customized key is incorrect, then the IC card is rejected or confiscated by the IC card reader/writer as being forged or illegally used.

In conclusion, the IC card system is designed to execute password checking after visually checking is made as to whether a card user is an authorized card owner, and then to allow the photograph data to be read from the IC card memory and the photograph image to be displayed on the basis of the photograph data. The displayed photograph image is compared with the photograph printed on the IC card, thereby checking the legitimacy of the IC card. Then, the personal authentication data is extracted from the photograph data using a customized key. The extracted data is then displayed. The displayed personal data is compared with the card user's personal data, thereby confirming that the presented IC card is a legitimate card.

As evidenced by the above, apparent image data contains other image data, acoustic data, and text data, all of which are present in a visually imperceptible manner. These embedded data are checked to confirm that the card user and the card are both legitimate.

Pursuant to the present invention, since the third party cannot recognize the presence of the inherent data, or rather the secret data, the information card with a high level of security is achievable.

According to the present invention, the inherent data is possible to verify the legitimacy of the information card. It is possible to hide the presence of the legitimacy data and the card owner data.

According to the present invention, the password enables protection of the information data, with a consequential increase in security of the card.

According to the present invention, the customized key can protect the inherent data.

According to the present invention, the information data can be protected against retrieval by password checking.

According to the present invention, unauthorized persons can be prevented from extracting the inherent data, thereby providing a high level of security.

Pursuant to the present invention, the information card can be prevented from being illegally used by means of the password and customized key.

Pursuant to the present invention, it is possible to provide triple security, and thus

to eliminate forgery and illegal use of the information card.

According to the present invention, the inherent data is embedded according to stegnanography, and is thus difficult to decrypt. As a result, the inherent data can securely be hidden.

According to the present invention, various files can be embedded in the inherent data.

According to the present invention, it is possible to construct an information card, which works as a memory card or an IC card, and a system of such an information card. In addition, an inexpensive card reader/writer can be provided.

Finally, pursuant to the present invention, the image data can be checked against the photograph. The photograph can be prevented from being forged.

What is claimed is:

1. An information card system including an information card (100) that includes a memory that stores information data, wherein the information card system is characterized by the fact that:

the information data includes one of image data and acoustic data;

the information data contains inherent data that is embedded in the information data according to a steganographic information hiding technique; and

the inherent data is data that authenticates the legitimacy of a card owner of the information card.

2. An information card system according to claim 1, wherein the memory stores a password for permitting the information data to be read from the memory.

3. An information card system according to claims 1 or 2, wherein the information card employs a customized key in order to give a permission to extract the inherent data from the information data.

4. An information card system according to claims 1 or 2, wherein the inherent data is embedded according to a steganographic information hiding technique by the steps of converting one of image data and acoustic data, both formed as information data, to pure binary code data, or converting the pure binary code data to canonical gray code data, decomposing one of the pure binary code data and the canonical gray code data into bit planes, segmenting the bit planes into regions according to a complexity measure, and replacing complex region-forming data with the inherent data.

5. An information card system according to claim 4, wherein the inherent data to be embedded is subject to a conjugation operation that produces a conjugated image in which the foreground area is identical in shape to the foreground area of the original image, the foreground area has a checkerboard pattern, and the background area has an inverse checkerboard pattern.

6. An information card system according to claim 1, wherein the memory comprises an IC chip.

7. An information card system according to claim 1 wherein the information card carries a photograph on a surface thereof, and the information data or

the inherent data is image data representing by the photograph.

8. An information card system according to claim 1, further comprising a data terminal (200) including input means for submitting a password, wherein the memory stores a password for permitting the information data to be read from the memory; and the data processing terminal (200) includes output means for outputting the read information data.

9. The information card system as claimed in claim 1, further comprising a data terminal (200), wherein the data terminal (200) includes input means for submitting a customized key, and inherent data extracting means for extracting the inherent data with the use of the submitted customized key.

10. An information card system according to claim 9, wherein the data terminal (200) includes password checking means for checking the submitted password against the password stored in the information card (100) to permit the information data to be read from the memory.

11. An information card system according claim 9, wherein the extracted inherent data is wholly or partly checked against inherent data read from a host (300) or inherent data entered from an external source.

12. An information card system according to claim 11, wherein the inherent data is embedded according to a steganographic information hiding technique by the steps of converting one of image data and acoustic data, both formed as information data, to pure binary code data, or converting the pure binary code data to canonical gray code data, decomposing one of the pure binary code data and the canonical gray code data into bit planes, segmenting the bit planes into regions according to a complexity measure, and replacing complex region-forming data with the inherent data.

13. An information card system according to claim 12, wherein the inherent data to be embedded is subject to a conjugation operation that produces a conjugated image in which the foreground area is identical in shape to the foreground area of the original image, the foreground area has a checkerboard pattern, and the background area has an inverse checkerboard pattern.

14. An information card system according to claim 8, wherein the memory comprises an IC chip.

15. An information card system according to claim 8, wherein the information card (100) carries a photograph on a surface thereof, and the information data or inherent data is image data representing the photograph.

M-H

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION** see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
1270-028		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US 99/ 21663	17/09/1999	29/09/1998
Applicant		
KAWAGUCHI, Eiji et al.		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 2 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

a. With regard to the **language,** the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

[ ] the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :

[ ] contained in the international application in written form.

[ ] filed together with the international application in computer readable form.

[ ] furnished subsequently to this Authority in written form.

[ ] furnished subsequently to this Authority in computer readble form.

[ ] the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

[ ] the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. [ ] **Certain claims were found unsearchable** (See Box I).

3. [ ] **Unity of invention is lacking** (see Box II).

4. With regard to the **title,**

[X] the text is approved as submitted by the applicant.

[ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**

[X] the text is approved as submitted by the applicant.

[ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No. 1

[X] as suggested by the applicant.

[ ] because the applicant failed to suggest a figure.

[ ] because this figure better characterizes the invention.

[ ] None of the figures.

INTERNATIONAL SEARCH REPORT

International Application No
[redacted]/US 99/21663

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06K19/07 G07C9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06K H04N G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 636 292 A (RHOADS GEOFFREY B) 3 June 1997 (1997-06-03) column 2, line 10 - line 16; figure 24 column 57, line 30 -column 58, line 45	1-7,11, 12
Y	EP 0 334 616 A (LEIGHTON FRANK T ;MICALI SILVIO (US)) 27 September 1989 (1989-09-27) column 5, line 21 -column 6, line 2; figure 1	1-7,11, 12
Y	US 5 689 587 A (MORIMOTO NORISHIGE ET AL) 18 November 1997 (1997-11-18) the whole document	1-7,11, 12
Y	EP 0 638 880 A (AUDIO DIGITALIMAGING INC) 15 February 1995 (1995-02-15) the whole document	1-7,11, 12

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 January 2000	20/01/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Chiarizia, S

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
/US 99/21663

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5636292 A	03-06-1997	US 5841978 A	24-11-1998
		US 5832119 A	03-11-1998
		US 5841886 A	24-11-1998
EP 0334616 A	27-09-1989	US 4879747 A	07-11-1989
		CA 1311559 A	15-12-1992
		DE 68918971 D	01-12-1994
		JP 2028775 A	30-01-1990
		US 4995081 A	19-02-1991
US 5689587 A	18-11-1997	US 5870499 A	09-02-1999
EP 0638880 A	15-02-1995	DE 69324915 D	17-06-1999
		DE 69324915 T	02-12-1999